PATENT
Attorney Docket No.: 784-51 (SI-19122-US)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS: Kyun-hun JANG, et al.

SERIAL NO.: not yet assigned

FILED: concurrent herewith **DATED:** June 26, 2003

FOR: METHOD USING ACCESS AUTHORIZATION DIFFERENTIATION IN WIRELESS ACCESS NETWORK AND SECURE ROAMING METHOD THEREOF

Mail Stop Patent Application
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF PRIORITY DOCUMENT

Sir:

Enclosed is a certified copy of Korean Patent Application No. 38882 filed on July 5, 2002, and from which priority is claimed under 35 U.S.C. § 119.

Respectfully submitted,

Paul J. Farrell
Reg. No. 33,494
Attorney for Applicant(s)

DILWORTH & BARRESE, LLP
333 Earle Ovington Blvd.
Uniondale, NY 11553
TEL: (516) 228-8484
FAX: (516) 228-8516
PJF/JK/lah

CERTIFICATION UNDER 37 C.F.R. § 1.10

I hereby certify that this correspondence (and any document referred to as being attached or enclosed) is being deposited with the United States Postal Service in an envelope as "Express Mail Post Office to Addressee" Mail Label Number EV333230662US addressed to: Mail Stop Patent Application, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on June 26, 2003.

Dated: June 26, 2003

Jeff Kirshner

KOREAN INTELLECTUAL PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

Application Number:	Patent Application No. 2002-38882
Date of Application:	5 July 2002
Applicant(s):	Samsung Electronics Co., Ltd.

12 May 2003

COMMISSIONER

[Document Name] Patent Application

[Application Type] Patent

[Receiver] Commissioner

[Reference No.] 0009

[Filing Date] 2002.07.05

[IPC] H04Q

[Title] Method using access right differentiation in wireless access network, and secure roaming method thereby

[Applicant]

[Name] Samsung Electronics Co., Ltd.
[Applicant code] 1-1998-104271-3

[Attorney]

[Name] Young-pil Lee
[Attorney's code] 9-1998-000334-6
[General Power of Attorney Registration No.] 1999-009556-9

[Attorney]

[Name] Hae-young Lee
[Attorney's code] 9-1999-000227-4
[General Power of Attorney Registration No.] 2000-002816-9

[Inventor]

[Name] JANG, Kyung Hun
[I.D. No.] 700228-1405318
[Zip Code] 442-470
[Address] 621-601 Sinnamusil Dongbo Apt., 968 Youngtong-dong Paldal-gu, Suwon-city, Kyungki-do
[Nationality] Republic of Korea

[Inventor]

[Name] LEE, In Sun
[I.D. No.] 711028-2030218

[Zip Code]	140-731
[Address]	9-1102 Cheonghwa Apt., Itaewon 2-dong Yongsan-gu, Seoul
[Nationality]	Republic of Korea

[Inventor]

[Name]	PARK, Jong Ae
[I.D. No.]	650814-2453511
[Zip Code]	137-930
[Address]	346-203 Banpo Jugong Apt., Banpo 1-dong Seocho-gu, Seoul
[Nationality]	Republic of Korea

[Request for Examination] Requested

[Application Order] I/We file as above according to Art. 42 of the Patent Law.
Attorney Young-pil Lee
Attorney Hae-young Lee

[Fee]

[Basic page]	20 Sheet(s)	29,000 won
[Additional page]	3 Sheet(s)	3,000 won
[Priority claiming fee]	0 Case(s)	0 won
[Examination fee]	0 Claim(s)	0 won
[Total]	32,000 Won	

[Enclosures]

1. Abstract and Specification (and Drawings)_1 copy

Kyung-hun JANG, ETAL
ATTY. DOCKET: 784-51
(SI-19122-US)

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0038882
Application Number

출 원 년 월 일 : 2002년 07월 05일
Date of Application JUL 05, 2002

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 05 월 12 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0009
【제출일자】	2002.07.05
【국제특허분류】	H04Q
【발명의 명칭】	링크 접속권한을 등급화 한 암호화 키 차등분배방법 및 이를 이용한 로밍방법
【발명의 영문명칭】	Method using access right differentiation in wireless access network, and secure roaming method thereby
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	장경훈
【성명의 영문표기】	JANG,Kyung Hun
【주민등록번호】	700228-1405318
【우편번호】	442-470
【주소】	경기도 수원시 팔달구 영통동 968 신나무실 동보아파트 621동 601호
【국적】	KR
【발명자】	
【성명의 국문표기】	이인선
【성명의 영문표기】	LEE,In Sun
【주민등록번호】	711028-2030218

【우편번호】 140-731
【주소】 서울특별시 용산구 이태원2동 청화아파트 9동 1102호
【국적】 KR
【발명자】
【성명의 국문표기】 박종애
【성명의 영문표기】 PARK,Jong Ae
【주민등록번호】 650814-2453511
【우편번호】 137-930
【주소】 서울특별시 서초구 반포1동 반포주공아파트 346동 203호
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 이해영 (인)
【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	3	면	3,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원
【합계】	32,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 무선 접속망에서의 암호화 키(encryption key) 분배방법과 로밍방법에 관한 것으로, 구체적으로는 로밍(roaming)시에 무선 접속망에서의 링크 접속 권한 등급에 따라서 미리 암호화 키를 차등 분배하여 빠른 로밍(roaming)을 수행할 수 있는 암호화 키 분배방법과 분배받은 암호화 키를 사용한 로밍방법에 관한 것이다. 본 발명의 암호화 키 분배방법은 현재 가지고 있는 암호화 키를 가지고는 통신할 수 없는 액세스 포인트와 통신하고자 하는 명령을 받는 제1단계, 상기 액세스 포인트의 링크접속권한을 판단하는 제2단계, 미리 획득한 암호화 키 세트에서 상기 판단한 링크접속권한에 대응되는 암호화 키를 선택하는 제3단계 및 상기 선택한 암호화 키를 사용하여 전송할 메시지를 암호화하여 상기 액세스 포인트와 통신하는 제4단계를 구비한다. 상기의 방법을 사용하면, 무선단말이 이동할 때 암호화 키 분배로 인해 지연되는 시간을 단축시켜 로밍(roaming) 또는 핸드오프(hand-off)를 빠르고 안전하게 이룸으로써 사용자의 편리성과 데이터 전송의 안전을 도모할 수 있는 효과가 있다.

【대표도】

도 3

【명세서】

【발명의 명칭】

링크 접속권한을 등급화 한 암호화 키 차등분배방법 및 이를 이용한 로밍방법{Method using access right differentiation in wireless access network, and secure roaming method thereby}

【도면의 간단한 설명】

도 1은 일반적인 암호화 키 사용방법을 나타낸 도면.

도 2는 본 발명의 암호화 키 사용방법을 나타낸 도면.

도 3은 본 발명의 초기 인증시에 암호화 키를 할당받는 방법 흐름도면.

도 4는 링크 접속 권한 별 암호화를 위한 패킷 헤더구조를 나타낸 도면.

도 5는 링크 접속 권한 별 암호화 키 할당장치를 나타낸 도면.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 무선 접속망에서의 암호화 키(encryption key) 분배방법에 관한 것으로, 구체적으로는 로밍(roaming)시에 무선 접속망에서의 링크 접속 권한 등급에 따라서 미리 암호화 키(encryption key)를 차등 분배하여 빠른 로밍(roaming)을 수행할 수 있는 암호화 키(encryption key) 분배방법과 분배받은 암호화 키를 사용한 로밍방법에 관한 것이다.

<7> 무선 접속망에서는 데이터의 기밀성(confidentiality)을 보장하고, 사용자 인증을 위해서 데이터를 암호화하여 전송한다. 암호화를 수행하기 위해서 암호화 키(encryption key)가 사용되어야 하는데, 현재 사용되고 있는 무선 접속망에서는 이 암호화 키(encryption key)를 무선 단말과 액세스 포인트(Access Point, AP)가 미리 공유하도록 되어 있다.

<8> 그러나 무선랜의 사용자가 점점 증가하고 있고 로밍(roaming) 또는 핸드오프(hand-off) 시에 이 암호화 키(encryption key) 교환을 위해 걸리는 시간이 길어지고 있어, 무선랜의 이동성을 고려할 때 종래의 암호화 키 (encryption key) 교환방법은 사용자의 불편함을 초래한다.

<9> 따라서 로밍(roaming) 또는 핸드오프(hand-off) 시에 암호화 키(encryption key) 교환으로 인한 지연시간을 최소화하는 것이 바람직하다. 이를 위해, 무선망은 사용자의 속성상 링크 접속시 접속등급이 존재할 수 있으므로 링크 접속 권한별로 암호화 키(encryption key)를 차등화시키는 것이 바람직하다.

<10> 무선 접속망에서는 무선 링크에서의 암호화를 수행하기 위해 해당 단말(station, STA)들이 암호화 키(encryption key)를 액세스 포인트(AP)와 공유하며, 무선 단말(STA)이 액세스 포인트(AP)간 로밍(roaming) 또는 핸드오프(hand-off) 시에는 액세스 포인트(AP)로부터 암호화에 사용되는 공유키(shared key)를 얻는 과정을 수행해야 한다. 이때, 무선 단말(STA)의 이동시 빠르고 안전한 로밍(fast secure roaming)의 가장 큰 걸림돌은 암호화 키(encryption key) 교환으로 인한 지연시간이다.

<11> 종래에는 광역 통신망(Wide Area Network, WAN)과 근거리 통신망(Local Area

Network, LAN), 액세스 포인트(AP) 및 무선단말(STA)로 구성된 무선망에서 한 액세스 포인트(AP)에 연결되어 있는 무선단말들은 모두 동일한 암호화 키(encryption key)를 사용한다. 따라서, 동일한 근거리 통신망(LAN)내에 속해있는 다른 액세스 포인트(AP)와 연결하거나, 다른 근거리 통신망(LAN)에 속해있는 액세스 포인트(AP)와 연결할 때도 다른 암호화 키(encryption key)를 사용하여야 하므로 로밍(roaming) 또는 핸드오프(hand-off) 시마다 해당하는 암호화 키(encryption key)를 다시 받아야 한다.

<12> 따라서, 이와 같은 종래의 방식에서는 무선단말(STA)이 액세스 포인트(AP)간 로밍(roaming) 또는 핸드오프(hand-off) 시마다 액세스 포인트(AP)로부터 암호화에 사용되는 암호화 키(encryption key)를 얻는 과정을 수행해야 한다. 그러므로, 무선 단말(STA)의 이동시 빠르고 안전한 로밍(fast secure roaming)을 수행하는데 어려움이 있었다.

【발명이 이루고자 하는 기술적 과제】

<13> 상기한 문제를 해결하기 위해 본 발명에서는, 액세스 포인트의 링크접속권한을 미리 설정하고, 상기 링크접속권한의 종류에 따라서 암호화 키를 달리하고, 상기 달리한 암호화 키를 무선단말이 미리 획득하도록 하여, 빠르고 안전한 로밍(fast secure roaming) 기능을 수행하는데 있어 암호화 키(encryption key) 교환으로 인해 생기는 지연시간을 최소화하는 것을 목적으로 한다.

【발명의 구성 및 작용】

<14> 상기한 목적을 이루기 위하여 본 발명에서는, 액세스 포인트의 링크접속권한을 미리 설정하고, 상기 링크접속권한의 종류에 따라서 암호화 키를 달리하고, 상기 달리한

암호화 키를 무선단말이 미리 획득하도록 하는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법을 제공한다.

<15> 상기한 목적을 이루기 위하여 본 발명에서는, 무선단말이 액세스 포인트에게 인증을 요구하고, 인증을 요구받은 상기 액세스 포인트가 상기 액세스 포인트의 링크접속권한을 판단하는 단계; 상기 판단결과에 따라 암호화 키를 획득하여 상기 암호화 키를 모아놓은 공유 키 세트를 생성하는 단계; 상기 무선단말이 랜 인증서버에게 인증을 요구하고, 인증을 요구받은 상기 랜 인증서버가 상기 랜에 속해있는 액세스 포인트의 링크접속권한을 판단하는 단계; 상기 판단결과에 따라 암호화 키를 획득하고 획득한 암호화 키를 상기 공유 키 세트에 추가하여 갱신하는 단계; 상기 무선단말이 광역 통신망 인증서버에게 인증을 요구하고, 인증을 요구받은 상기 광역 통신망 인증서버가 상기 광역 통신망에 속해있는 액세스 포인트의 링크접속권한을 판단하는 단계; 및 상기 판단결과에 따라 암호화 키를 획득하고 획득한 암호화 키를 상기 공유 키 세트에 추가하여 갱신하는 단계를 포함하는 링크접속권한 등급별 암호화 키 할당방법을 제공한다.

<16> 상기한 목적을 이루기 위하여 본 발명에서는, 액세스 포인트의 링크접속권한을 미리 설정하고, 상기 링크접속권한의 종류에 따라서 암호화 키를 달리하고, 상기 달리한 암호화 키를 액세스 포인트별로 각각 받아 암호화 키 세트를 무선단말이 미리 획득하는 단계; 상기 암호화 키 세트에서 현재 선택한 암호화 키를 가지고는 통신할 수 없는 액세스 포인트와 통신하고자 하는 명령을 받는 단계; 상기 통신할 수 없는 액세스 포인트의 링크접속권한을 판단하는 단계; 상기 미리 획득한 암호화 키 세트에서 상기 판단한 링크접속권한에 대응되는 암호화 키를 선택하는 단계; 및 상기 선택한 암호화 키를 사용하여

전송할 메시지를 암호화하여 상기 통신할 수 없는 액세스 포인트와 통신하는 단계를 포함하는 링크접속권한 등급별 암호화 키 할당을 이용한 무선단말의 로밍방법을 제공한다.

<17> 상기한 목적을 이루기 위하여 본 발명에서는, 상기 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<18> 상기한 목적을 이루기 위하여 본 발명에서는, 무선단말의 어느 액세스 포인트와 통신하기 위한 접속 허용 권한의 등급을 판단하는 링크접속권한 판단부; 상기 등급에 따른 암호화 키를 미리 저장하고 있는 암호화 키 저장부; 및 상기 정보접속권한 판단부에서의 판단결과에 대응되는 등급의 암호화 키를 상기 암호화 키 저장부로부터 읽어들여 그 값을 상기 무선단말에게 전달하는 암호화 키 할당부를 포함하는 링크접속권한 등급별 암호화 키 할당장치를 제공한다.

<19> 상기한 목적을 이루기 위하여 본 발명에서는, 무선단말, 액세스 포인트를 포함하는 무선망에서, 상기 무선망에서 전송되는 데이터 패킷의 헤더; 상기 무선단말이 상기 액세스 포인트와 통신하기 위하여 접속할 수 있는 권한을 나타내는 링크접속 권한정보 저장필드; 전송될 데이터의 내용이 암호화 되어 저장되어 있는 암호화 데이터 필드; 및 상기 데이터의 전송시 상기 데이터의 오류를 정정하는데 사용되는 오류정정필드를 구비하는 링크접속권한 등급별 암호화 키 할당을 위한 무선통신 패킷 자료 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<20> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<21> 도 1은 일반적인 암호화 키 사용방법을 나타낸 도면이다.

<22> 광역 통신망(WAN)과 근거리 통신망(LAN), 액세스 포인트(AP) 및 무선단말(STA)로 구성된 무선망을 가정하자. 여기서 광역 통신망(WAN)은 지리적으로 흩어져 있는 통신망을 의미하는 것으로서 근거리 통신망(LAN)과 구별하여 보다 넓은 지역을 커버하는 통신 구조를 나타내는 용어로 사용된다. 보통 근거리 통신망(LAN)의 범위는 1개의 빌딩이나 학교, 연구소 및 생산공장 등의 일정 구역내인 것에 반해, 광역 통신망(WAN)은 넓은 지역을 연결하는 네트워크를 지칭하는 것으로 지방과 지방, 국가와 국가, 또는 대륙과 대륙 등과 같이 지리적으로 완전하게 떨어져 있는 장거리 지역 사이를 연결하고 있는 통신망이다.

<23> 도면에서 보는 바와 같이 어느 한 액세스 포인트(AP)에 연결되어 있는 무선단말들은 모두 동일한 암호화 키(encryption key)를 사용한다. 예를 들어 액세스 포인트 1-1(AP1-1)(101)에 연결되어 있는 무선단말은 암호화 키(encryption key) #1-1(111)을 사용하고, 액세스 포인트1-2(AP1-2)(102)에 연결되어 있는 무선단말은 암호화 키(encryption key) #1-2(112)를 사용한다. 따라서 무선단말1(STA1)(131), 무선단말2(STA2)(132), 무선단말3(STA3)(133) 모두 암호화 키(encryption key) #1-2(112)를 사용한다.

<24> 동일한 근거리 통신망(LAN)내의 다른 액세스 포인트(AP)와 연결하거나, 다른 근거리 통신망(LAN)내의 액세스 포인트(AP)와 연결할 때도 다른 암호화 키(encryption key)를 사용하여야 하므로 로밍(roaming) 또는 핸드오프(hand-off) 시마다 해당하는 암호화 키(encryption key)를 다시 받아야 한다. 예를 들어 무선단말1(STA1)(131)이 다른 근거리 통신망2(LAN2)(140)에 속해 있는 액세스 포인트2-3(AP2-3)(141)과 통신하기 위해서는 가지고 있던 암호화 키 #1-2 대신에 새로운 암호화 키 #2-3(141)을 받아야 한다.

<25> 도 2는 본 발명의 암호화 키 사용방법을 나타낸 도면이다.

<26> 본 발명에서 제안하는 등급별 암호화 키(encryption key)를 사용하기 위해서 링크 접속 권한 등급이 존재한다. 암호화 키(encryption key)는 모두 4개의 등급으로 나누어져 있다.

<27> 등급1은 그 무선단말(STA)이 소속되어 있는 액세스 포인트(AP)로의 접속 허용 권한, 등급2는 그 무선단말(STA)이 소속되어 있는 근거리 통신망(LAN)에 속한 특정 액세스 포인트(AP)들로의 접속 허용 권한, 등급3은 그 무선단말(STA)이 소속되어 있는 근거리 통신망(LAN)에 속한 모든 액세스 포인트(AP)들로의 접속 허용 권한, 그리고 등급4는 광역 통신망(WAN)에 속한 다수의 액세스 포인트(AP)들로의 접속 허용 권한이다.

<28> 그리고, 초기 인증시 각 무선단말(STA)이 가질 수 있는 모든 암호화 키(encryption key)를 미리 획득한다. 예를 들어, 무선단말1(STA1)(210)이 액세스 포인트 1-2(AP1-2)(220)와 통신하기 위해서는 등급1의 암호화 키 #1(221) 이 필요하고, 액세스 포인트1-3(AP1-3)(230)과 통신하기 위해서는 등급2의 암호화 키 #2(231) 이 필요하고, 액세스 포인트1-4(AP1-4)(240)와 통신하기 위해서는 등급3의 암호화 키 #3(241) 이 필요하다. 그리고 다른 근거리 통신망2(LAN2)(250)에 속해있는 액세스 포인트 2-2(AP2-2)(251)와 통신하기 위해서는 등급4의 암호화 키 #4(252) 가 필요하다. 따라서, 무선단말1(STA1)(210)은 그 등급에 따라서 이들 4개의 암호화 키 세트 {암호화 키 #1, 암호화 키 #2, 암호화 키 #3, 암호화 키 #4}(260)를 획득한다.

<29> 이들 등급에는 우선 순위가 있는데, 정보 접속 권한은 등급1 > 등급2 > 등급3 > 등급4 의 순이고, 망 사용 권한은 등급1 < 등급2 < 등급3 < 등급4 의 순이다. 정보 접속 권한은 여러개의 무선단말이 동시에 접속한 경우 어떤 등급을 가진 무선단말(STA)이 그

액세스 포인트(AP)를 먼저 이용할 수 있도록 하는가를 말하는 것이고, 망 사용 권한은 망을 더 많이 사용할 수 있는 권한을 말한다. 즉, 등급 4는 모든 액세스 포인트(AP)와 통신할 수 있는 것이므로 더 높은 권한을 갖게 된다. 그리고 암호화 키(encryption key)는 등급별로 차등화 되어 다른 키를 갖게 되며 단말 초기 인증 절차시 자신의 무선단말(STA)에게 해당되는 등급의 암호화 키(encryption key)들을 미리 할당받는다.

<30> 하나의 무선단말(STA)이 하나의 액세스 포인트(AP)에서 다른 액세스 포인트(AP), 또는 다른 근거리 통신망(LAN)으로 이동할 때 처음 로밍(roaming) 시에 할당받은 공유키 세트(shared key set)에서 암호화 키(encryption key)를 적절히 선택하여 암호화를 수행한다. 이렇게 함으로써 다른 액세스 포인트(AP) 나 근거리 통신망(LAN)으로 로밍(roaming)하기 위해서 수행하여야 할 키 교환으로 인해 지연되는 시간을 줄일 수 있다

<31> 도 3은 초기 인증시에 본 발명의 암호화 키를 할당받는 방법 흐름도면이다.

<32> 즉, 본 발명의 무선 접속망에서의 링크 접속 권한 등급화에 따른 암호화 키(encryption key) 차등화 방법을 이용하기 위하여 초기 인증시에 암호화 키(encryption key)를 할당받는 방법을 나타낸 흐름도이다.

<33> 등급별 암호화 키(encryption key)를 할당하기 위해서는 액세스 포인트(AP), 근거리 통신망(LAN), 광역 통신망(WAN)으로 구성된 무선망에서 하나의 무선단말(STA)(310)이 액세스 포인트(AP)(320)에 접근하면서 인증을 요구한다(350). 무선단말(STA)(310)과 액세스 포인트(AP)(320)가 공유하는 암호화 키(encryption key)세트를 공유 키 세트(Shared Key, SK)라고 한다.

<34> 액세스 포인트(AP)(320)는 인증 절차를 거쳐, 인증이 되면 등급1에 해당하는 가를 판단하여(351), 등급1에 해당하면 공유 키 SK={SK1} 을 생성하고(352), 그렇지 않으면 SK={null}로 한다(353). 그리고 나서 LAN 인증 서버(330)에 무선단말(STA)(310)에 대한 인증을 요구한다(354).

<35> LAN 인증 서버(330)는 등급2에 해당하는지를 판단하고(355), 등급2에 해당하면 새로운 공유 키 SK2를 생성하고 기존의 공유 키 SK와 합하여 새로운 공유 키 세트 SK={SK1}U{SK2}를 구성한다(356). 그리고 나서 등급 3에 해당하는지를 확인하여(357) 등급3에 해당하면 새로운 공유 키 SK3을 생성하여 새로운 공유 키 세트 SK={SK1}U{SK2}U{SK3}를 구성한다(358). 이때, 기존의 공유 키 SK={null} 인 경우에는 전자에는 SK={SK2}, 후자에는 SK={SK2}U{SK3} 가 된다.

<36> 그리고 나서 LAN 인증 서버(330)는 WAN 인증서버(340)에게 무선단말(STA)(310)의 인증을 요구한다(359). 그러면 WAN 인증 서버(340)는 등급4에 해당하는가를 판단하여(360), 등급4에 해당하면 LAN 인증 서버(330)로부터 받은 공유 키 세트 SK 에 자신에 생성한 공유 키 SK4를 합하여 새로운 공유 키 세트 SK를 SK={SK1}U{SK2}U{SK3}U{SK4} 의 형태로 만들어(361) 인증을 완료하고, 이 공유 키 세트 SK 를 무선단말(STA)(310)에게 보낸다(362). 만약 WAN 인증 서버(340)에 의해서 인증이 되지 않는 경우는 LAN 인증 서버(330)로부터 받은 공유 키 세트 SK를 무선단말(STA)(310)에게 전달하며 인증을 완료하고, 만약 이 때까지 공유 키 세트 SK 가 SK={null} 이면 인증이 거절된다.

<37> 이렇게 등급별 암호화 키(encryption key)를 할당받고 나서, 이를 이용해 고속의 안전한 로밍(roaming)을 하는 방법은 도 2와 같다. 무선단말(STA)이 초기 인증시 획득한 공유 키 세트 SK를 가지고 자신이 속한 액세스 포인트(AP)와 데이터를 주고받을 때는

SK1을 이용해 데이터를 암호화한다. 이때 헤더의 링크 접속 권한 표시 방법은 도 4와 같다. 그리고 등급 2를 부여받은 액세스 포인트(AP)로 이동한 경우에는 암호화를 위해 SK2를 사용해야 한다.

<38> 마찬가지로, 같은 근거리 통신망(LAN) 상에서 등급 3의 권한이 있는 액세스 포인트(AP)로 이동하여 그 액세스 포인트(AP)와 통신하는 경우에는 SK3을 사용하고, 등급 4의 권한을 부여받은 근거리 통신망(LAN) 상의 액세스 포인트(AP)를 사용하는 경우에는 SK4를 사용하여 암호화를 수행한다. 각각의 경우에 헤더의 링크 접속 권한 표시 방법은 도 4와 같다.

<39> 도 4는 링크 접속 권한 별 암호화를 위한 패킷 헤더구조를 나타낸다.

<40> 도면과 같이 무선 전송망에서 송수신되는 패킷은 헤더(410), 링크접속 권한정보 저장필드(420), 암호화 데이터 필드(encrypted data)(430) 및 오류정정필드(CRC)(440)로 구성된다. 따라서, 전송되는 패킷의 헤더(410)에 링크접속 권한정보를 저장하는 필드(420)를 2 비트 할당하여 그 비트의 조합으로서 4개의 등급을 나타낼 수 있다. 예를 들어 "00"이면 등급1을, "01"이면 등급2를, "10"이면 등급3을, "11"이면 등급4를 나타낸다.

<41> 도 5는 링크 접속 권한 별 암호화 키 할당장치를 나타낸 도면이다.

<42> 암호화 키 할당장치는 링크접속권한 판단부(510), 암호화 키 저장부(520) 및 암호화 키 할당부(530)를 구비하고 있다.

<43> 링크접속권한 판단부(510)는 무선단말의 어느 액세스 포인트(AP)와 통신하기 위한 접속 허용 권한의 등급을 판단한다. 등급의 종류로는 상기 무선단말(STA)이 소속되어 있는 액세스 포인트(AP)로의 접속 허용 권한을 의미하는 등급1, 상기 무선단말(STA)이 소

속되어 있는 근거리 통신망(LAN)에 속한 특정 액세스 포인트(AP)들로의 접속 허용 권한을 의미하는 등급2, 상기 무선단말(STA)이 소속되어 있는 근거리 통신망(LAN)에 속한 모든 액세스 포인트(AP)들로의 접속 허용 권한을 의미하는 등급3 및 광역 통신망(WAN)에 속한 다수의 액세스 포인트(AP)들로의 접속 허용 권한을 의미하는 등급4가 있다.

<44> 어느 무선단말(STA)이 액세스 포인트(AP)로 인증을 요구하면 상기 정보접속권한 판단부(510)는 그 무선단말(STA)의 정보접속권한 등급을 판단한다.

<45> 암호화 키저장부(520)는 상기 등급에 따른 암호화 키를 미리 저장하고 있다.

<46> 암호화 키 할당부(530)는 상기 링크접속권한 판단부(510)에서의 판단결과에 대응되는 등급의 암호화 키를 상기 암호화 키 저장부(520)로부터 읽어들여 그 값을 무선단말(STA)에게 전달한다.

<47> 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

<48> 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 씨디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 포함한다.

<49> 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되

어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

【발명의 효과】

<50> 상술한 바와 같이 본 발명은, 링크 접속 권한 등급화에 따는 암호화 키(encryption key) 차등화 및 이를 이용한 빠르고 안전한 로밍(fast secure roaming) 방법을 사용함으로써 무선 접속망을 이용하는 이동단말이 이동할 때 암호화 키(encryption key) 분배로 인해 지연되는 시간을 단축시켜 로밍(roaming) 또는 핸드오프(hand-off)를 빠르고 안전하게 이룸으로써 사용자의 편리성과 데이터 전송의 안전을 도모할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

액세스 포인트의 링크접속권한을 미리 설정하고, 상기 링크접속권한의 종류에 따라서 암호화 키를 달리하고, 상기 달리한 암호화 키를 무선단말이 미리 획득하도록 하는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 2】

제1항에 있어서, 상기 링크접속권한은

상기 무선단말이 소속되어 있는 액세스 포인트로의 접속 허용 권한을 의미하는 등급1, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 특정 액세스 포인트들로의 접속 허용 권한을 의미하는 등급2, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 모든 액세스 포인트들로의 접속 허용 권한을 의미하는 등급3 및 광역 통신망에 속한 다수의 액세스 포인트들로의 접속 허용 권한을 의미하는 등급4로 나누어져 있는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 3】

제1항에 있어서, 상기 무선단말은

상기 암호화 키를 상기 링크접속권한에 대응되는 암호화 키를 복수개 가지고 있다가, 어느 액세스 포인트와 통신하고자 하는 경우 그 액세스 포인트의 링크접속권한에 대응되는 암호화 키를 상기 복수개의 암호화 키 중에서 선택하여 상기 액세스 포인트와 통신하는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 4】

(a) 무선단말이 액세스 포인트에게 인증을 요구하고, 인증을 요구받은 상기 액세스 포인트가 상기 액세스 포인트의 링크접속권한을 판단하는 단계;

(b) 상기 판단결과에 따라 암호화 키를 획득하여 상기 암호화 키를 모아놓은 공유 키 세트를 생성하는 단계;

(c) 상기 무선단말이 랜 인증서버에게 인증을 요구하고, 인증을 요구받은 상기 랜 인증서버가 상기 랜에 속해있는 액세스 포인트의 링크접속권한을 판단하는 단계;

(d) 상기 판단결과에 따라 암호화 키를 획득하고 획득한 암호화 키를 상기 공유 키 세트에 추가하여 갱신하는 단계;

(e) 상기 무선단말이 광역 통신망 인증서버에게 인증을 요구하고, 인증을 요구받은 상기 광역 통신망 인증서버가 상기 광역 통신망에 속해있는 액세스 포인트의 링크접속권한을 판단하는 단계; 및

(f) 상기 판단결과에 따라 암호화 키를 획득하고 획득한 암호화 키를 상기 공유 키 세트에 추가하여 갱신하는 단계를 포함하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 5】

제4항에 있어서, 상기 (a) 단계는

상기 무선단말이 액세스 포인트에게 인증을 요구하고, 요구받은 상기 액세스 포인트가 상기 액세스 포인트의 링크접속권한이 상기 무선단말이 소속되어 있는 액세스 포인트로의 접속 허용 권한을 의미하는 등급1에 해당하는가를 판단하는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 6】

제4항에 있어서, 상기 (c) 단계는

(c1) 상기 랜 인증서버가 상기 액세스 포인트의 링크접속권한이 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 특정 액세스 포인트들로의 접속 허용 권한을 의미하는 등급2에 해당하는가를 판단하는 단계;

(c2) 상기 판단결과 상기 등급2에 해당하면 상기 등급2의 암호화 키를 획득하고 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 모든 액세스 포인트들로의 접속 허용 권한을 의미하는 등급3에 해당하는가를 다시 판단하는 단계; 및

(c3) 상기 판단결과 상기 등급3에 해당하면 상기 등급3의 암호화 키를 획득하는 단계를 포함하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 7】

제6항에 있어서, 상기 (c2) 단계는

상기 판단결과 상기 등급2에 해당하지 않으면 아무런 암호화 키를 할당하지 않고 상기 등급3에 해당하는가를 다시 판단하고, 상기 등급3에도 해당하지 않으면 암호화 키를 할당하지 않는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당방법.

【청구항 8】

(a) 액세스 포인트의 링크접속권한을 미리 설정하고, 상기 링크접속권한의 종류에 따라서 암호화 키를 달리하고, 상기 달리한 암호화 키를 액세스 포인트별로 각각 받아 암호화 키 세트를 무선단말이 미리 획득하는 단계;

(b) 상기 암호화 키 세트에서 현재 선택한 암호화 키를 가지고는 통신할 수 없는 액세스 포인트와 통신하고자 하는 명령을 받는 단계;

(c) 상기 통신할 수 없는 액세스 포인트의 링크접속권한을 판단하는 단계;

(d) 상기 미리 획득한 암호화 키 세트에서 상기 판단한 링크접속권한에 대응되는 암호화 키를 선택하는 단계; 및

(e) 상기 선택한 암호화 키를 사용하여 전송할 메시지를 암호화하여 상기 통신할 수 없는 액세스 포인트와 통신하는 단계를 포함하는 링크접속권한 등급별 암호화 키 할당을 이용한 무선단말의 로밍방법.

【청구항 9】

제8항에 있어서, 상기 암호화 키 세트의 링크접속권한의 종류는

상기 무선단말이 소속되어 있는 액세스 포인트로의 접속 허용 권한을 의미하는 등급1, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 특정 액세스 포인트들로의 접속 허용 권한을 의미하는 등급2, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 모든 액세스 포인트들로의 접속 허용 권한을 의미하는 등급3 및 광역 통신망에 속한 다수의 액세스 포인트들로의 접속 허용 권한을 의미하는 등급4로 나누어져 있는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당을 이용한 무선단말의 로밍방법.

【청구항 10】

제1항 내지 제9항 중 어느 한 항에 기재된 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【청구항 11】

무선단말의 어느 액세스 포인트와 통신하기 위한 접속 허용 권한의 등급을 판단하는 링크접속권한 판단부;

상기 등급에 따른 암호화 키를 미리 저장하고 있는 암호화 키 저장부; 및

상기 정보접속권한 판단부에서의 판단결과에 대응되는 등급의 암호화 키를 상기 암호화 키 저장부로부터 읽어들여 그 값을 상기 무선단말에게 전달하는 암호화 키 할당부를 포함하는 링크접속권한 등급별 암호화 키 할당장치.

【청구항 12】

제11항에 있어서, 상기 등급은

상기 무선단말이 소속되어 있는 액세스 포인트로의 접속 허용 권한을 의미하는 등급1, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 특정 액세스 포인트들로의 접속 허용 권한을 의미하는 등급2, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 모든 액세스 포인트들로의 접속 허용 권한을 의미하는 등급3 및 광역 통신망에 속한 다수의 액세스 포인트들로의 접속 허용 권한을 의미하는 등급4인 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당장치.

【청구항 13】

무선단말, 액세스 포인트를 포함하는 무선망에서,

상기 무선망에서 전송되는 데이터 패킷의 헤더;

상기 무선단말이 상기 액세스 포인트와 통신하기 위하여 접속할 수 있는 권한을 나타내는 링크접속 권한정보 저장필드;

전송될 데이터의 내용이 암호화 되어 저장되어 있는 암호화 데이터 필드; 및 상기 데이터의 전송시 상기 데이터의 오류를 정정하는데 사용되는 오류정정필드를 구비하는 링크접속권한 등급별 암호화 키 할당을 위한 무선통신 패킷 자료 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체.

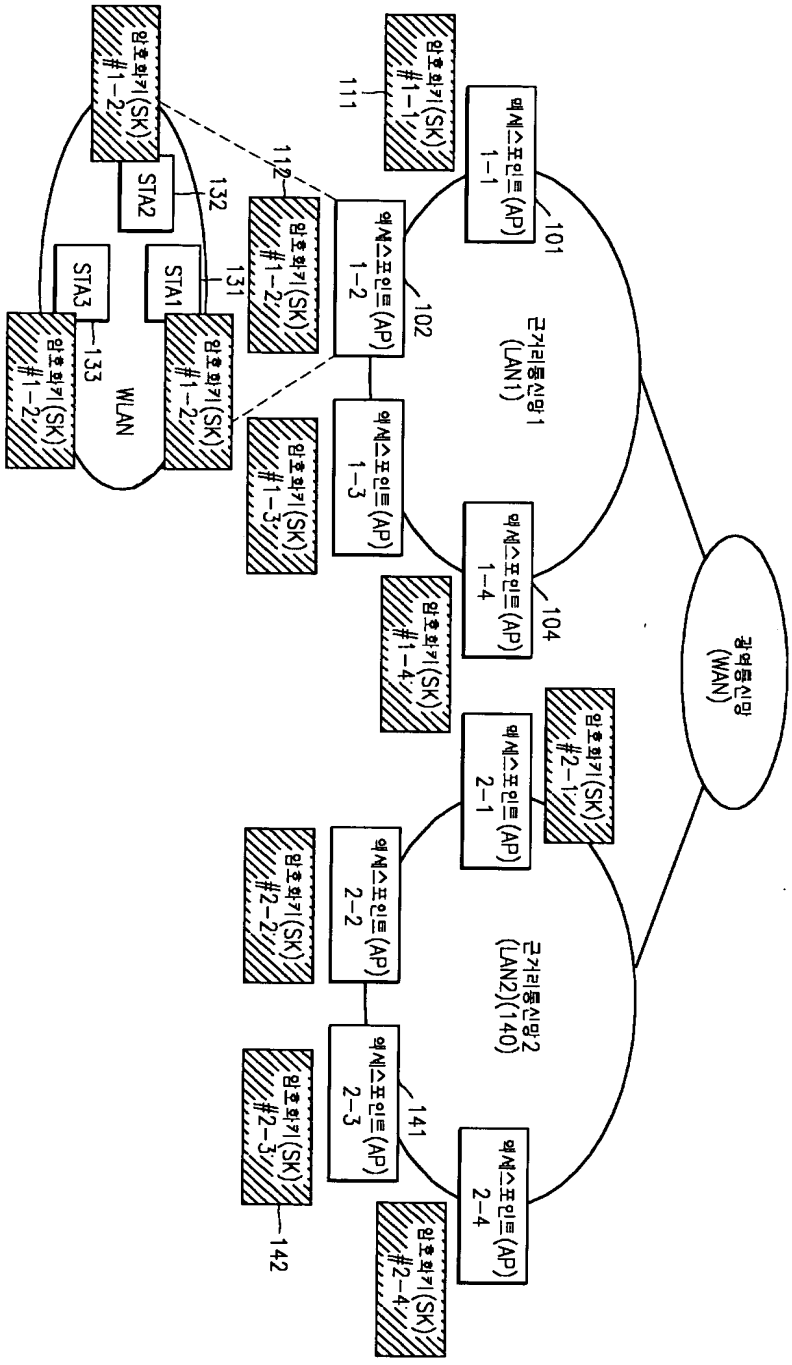
【청구항 14】

제13항에 있어서, 상기 링크접속 권한정보 저장필드는

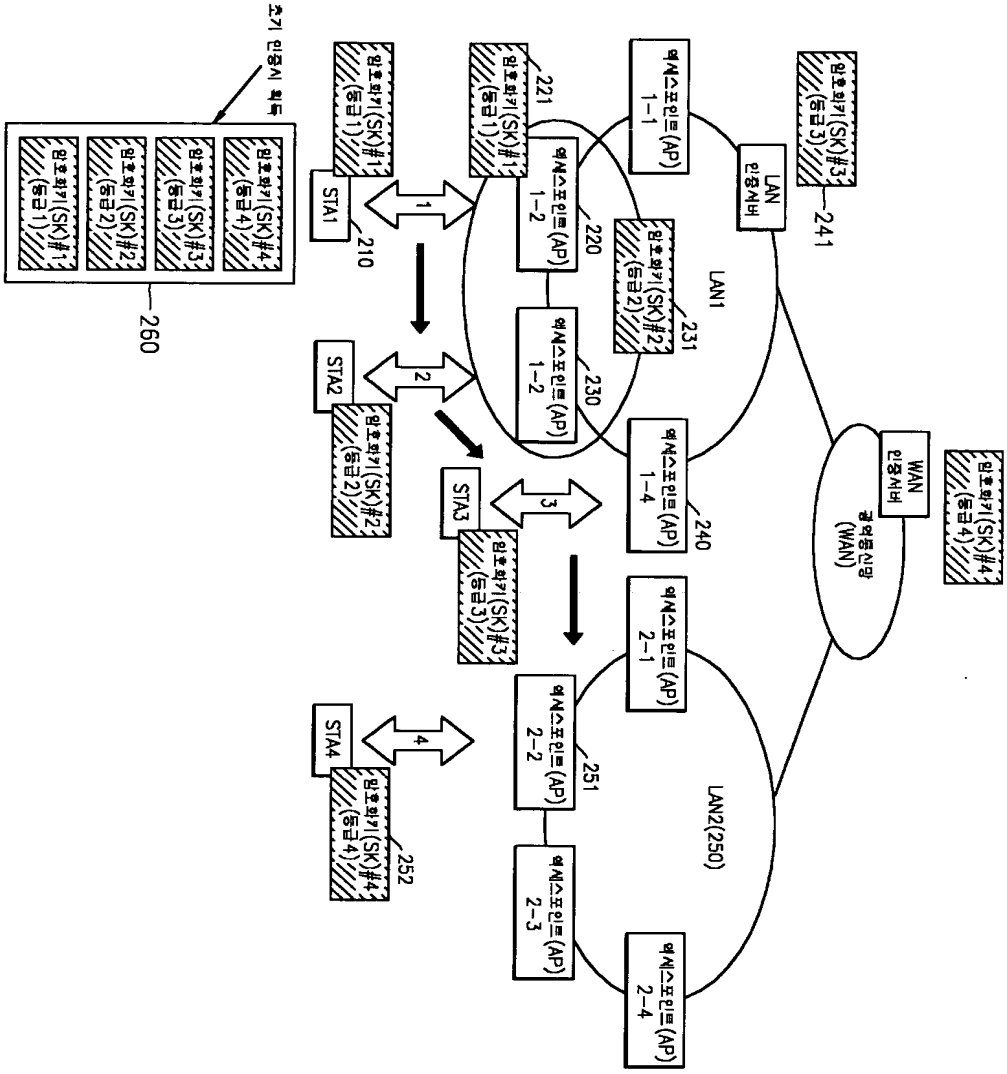
2비트로 구성되고 각 비트를 조합하여 상기 무선단말이 소속되어 있는 액세스 포인트로의 접속 허용 권한을 의미하는 등급1, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 특정 액세스 포인트들로의 접속 허용 권한을 의미하는 등급2, 상기 무선단말이 소속되어 있는 근거리 통신망에 속한 모든 액세스 포인트들로의 접속 허용 권한을 의미하는 등급3 및 광역 통신망에 속한 다수의 액세스 포인트들로의 접속 허용 권한을 의미하는 등급4를 나타내는 것을 특징으로 하는 링크접속권한 등급별 암호화 키 할당을 위한 무선통신 패킷 자료 구조를 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

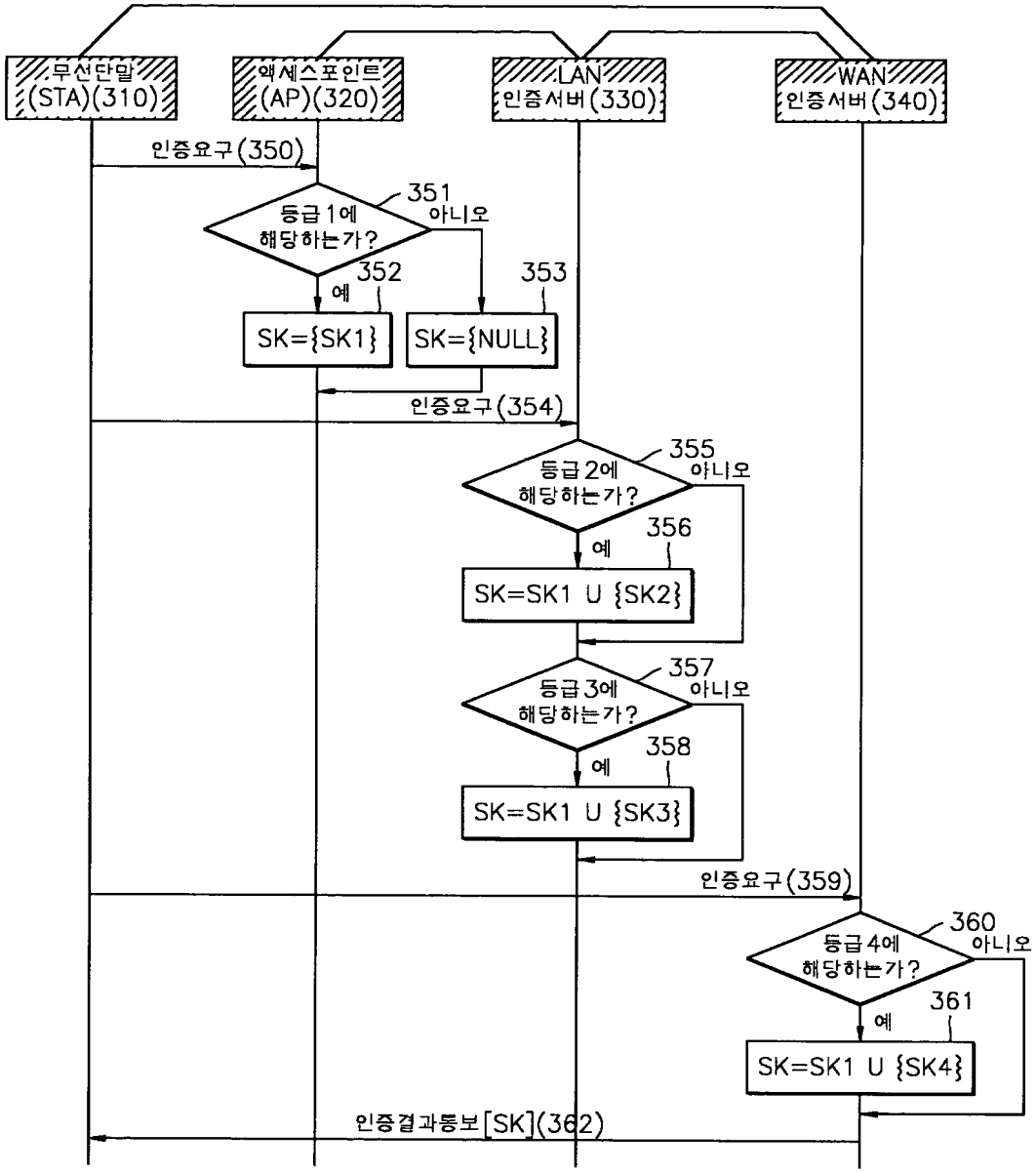
【도 1】


광역통신망
(WAN)
근거리통신망1
(LAN1)
근거리통신망2
(LAN2)(140)
WLAN
액세스포인트(AP)
1-1
액세스포인트(AP)
1-2
액세스포인트(AP)
1-3
액세스포인트(AP)
1-4
액세스포인트(AP)
2-1
액세스포인트(AP)
2-2
액세스포인트(AP)
2-3
액세스포인트(AP)
2-4
101
102
104
141
암호화키(SK)
#1-1
암호화키(SK)
#1-2
암호화키(SK)
#1-3
암호화키(SK)
#1-4
암호화키(SK)
#2-1
암호화키(SK)
#2-2
암호화키(SK)
#2-3
암호화키(SK)
#2-4
111
112
131
132
133
142
STA1
STA2
STA3

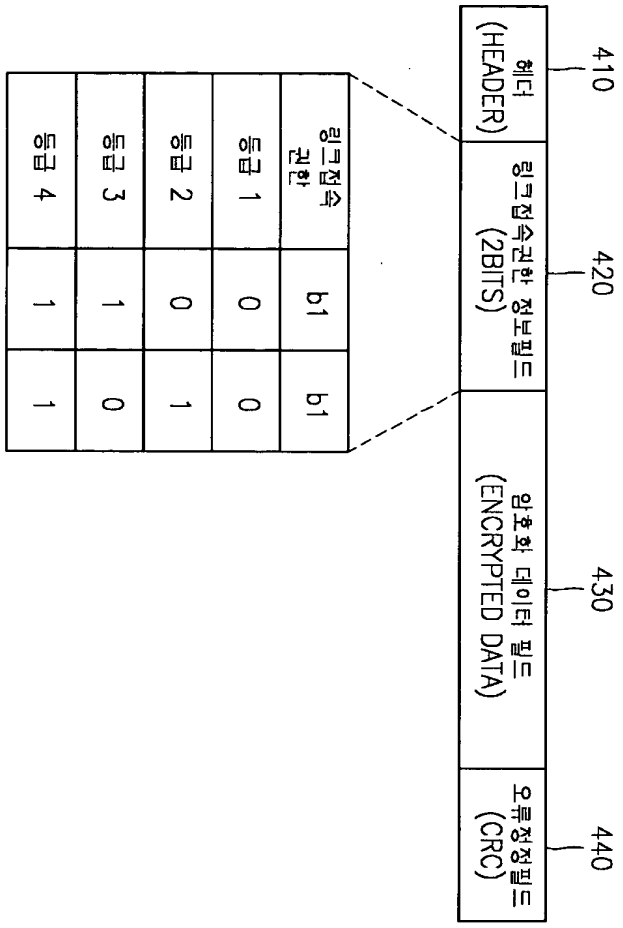
【도 2】


초기 인증시 획득
암호화키(SK)#1 (등급1)
암호화키(SK)#2 (등급2)
암호화키(SK)#3 (등급3)
암호화키(SK)#4 (등급4)
260
암호화키(SK)#1 (등급1)
STA1
210
1
암호화키(SK)#2 (등급2)
STA2
2
암호화키(SK)#3 (등급3)
STA3
3
암호화키(SK)#4 (등급4)
STA4
4
252
액세스포인트(AP) 2-4
액세스포인트(AP) 2-3
액세스포인트(AP) 2-2
251
액세스포인트(AP) 2-1
LAN2(250)
액세스포인트(AP) 1-4
240
액세스포인트(AP) 1-2
230
액세스포인트(AP) 1-2
220
221
암호화키(SK)#1 (등급1)
액세스포인트(AP) 1-1
암호화키(SK)#2 (등급2)
231
LAN1
LAN 인증서버
암호화키(SK)#3 (등급3)
241
WAN 인증서버
광역통신망 (WAN)
암호화키(SK)#4 (등급4)

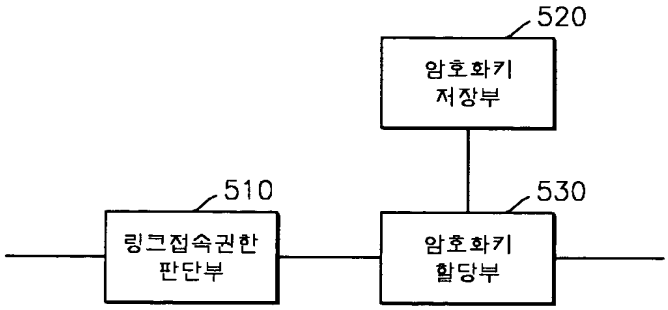
【도 3】


무선단말 (STA)(310)
액세스포인트 (AP)(320)
LAN 인증서버(330)
WAN 인증서버(340)
인증요구(350)
351
등급1에 해당하는가?
아니오
예
352
353
SK={SK1}
SK={NULL}
인증요구(354)
355
등급2에 해당하는가?
아니오
예
356
SK=SK1 U {SK2}
357
등급3에 해당하는가?
아니오
예
358
SK=SK1 U {SK3}
인증요구(359)
360
등급4에 해당하는가?
아니오
예
361
SK=SK1 U {SK4}
인증결과통보[SK](362)

【도 4】


헤더 (HEADER)
410
링크접속권한 정보필드 (2BITS)
420
암호화 데이터 필드 (ENCRYPTED DATA)
430
오류정정필드 (CRC)
440
링크접속 권한
등급 1
등급 2
등급 3
등급 4
b1
0
0
b1
1
0
1
1
0

【도 5】


520
암호화키 저장부
510
링크접속권한 판단부
530
암호화키 할당부